CSWG Comments on PAP01: Role of the Internet Protocol Suite (IPS) in the Smart Grid

Table of Contents

Tables

Introduction

In September 2010, the NIST Smart Grid Interoperability Panel (SGIP) Project Management Office (PMO) requested the NIST Cyber Security Working Group (CSWG) to review and provide input to Priority Action Plan (PAP) 01: Role of IP in the Smart Grid. PAP01 task 2 calls for the identification of a core set of Internet Protocol (IP) Suite specifications that can be used for Smart Grid. An Internet Engineering Task Force (IETF) draft document written by Fred Baker and Dave Meyer on "Core Protocols in the Internet Protocol Suite"[1] provided the core set of IP Suite (IPS) specifications and is the focus of this CSWG review. This CSWG review is a high level overview of the "Core Protocols in the Internet Protocol Suite" and provides cyber security recommendations for PAP01 task 2. This is not a formal CSWG standards review of the IPS protocols.

For interoperable networks, it is important to study the suitability of Internet networking technologies for smart grid applications. PAP01 task 2 investigated the capabilities of protocols and technologies in the IPS by working with key standards development organization (SDO) committees to determine the characteristics of each protocol for smart grid application areas and types. It addressed the question "What does the IETF consider to be the core components of the Internet Architecture?" The target audience for this IETF draft is people seeking guidance on how to construct appropriate IPS profiles for the Smart Grid.

What the IETF Draft Document Covers

- Discussion on common pitfalls and many of the relevant issues to consider when developing a network based on the IPS.
- Many of the key capabilities of existing IPS protocols and technologies.
- Normative (Appendix A) and informative (Appendix B) references which look at existing protocols in detail. Examples include Simple Network Management Protocol (SNMP).
- Specific protocol discussions. The specific protocols discussed within the document are in Table 1. The specific protocols are discussed as examples and reference other Request for Comment (RFC) documents.
- Recommendations on the available IPS protocols that are in current use and describe that use.

IETF Document Section	Protocol / Topic Mentioned
Security solutions	• Session identification, authentication, authorization, and accounting • IP Security Architecture (IPsec)

[1] http://tools.ietf.org/html/draft-baker-ietf-core-08, Fred Baker and Dave Meyer, September 18, 2009.

IETF Document Section	Protocol / Topic Mentioned
	• Transport Layer Security (TLS) • Secure/Multipurpose Internet Mail Extensions (S/MIME)
Network Layer	• IPv4/IPv6 Coexistence Advice • Internet Protocol Version 4 • Internet Protocol Version 6 • Routing for IPv4 and IPv6
Transport Layer	• User Datagram Protocol (UDP) • Transmission Control Protocol (TCP) • Stream Control Transmission Protocol (SCTP) • Datagram Congestion Control Protocol (DCCP)
Infrastructure	• Domain Name System • Dynamic Host Configuration
Network Management	• Simple Network Management Protocol (SNMP) • Network Configuration (NETCONF) Protocol
Service and Resource Discovery	• Service Discovery • Resource Discovery
Other applications	• Network Time • Session Initiation Protocol • Calendaring

Table 1 - Protocols Mentioned in Draft IETF Document

What the IETF Draft Document Does Not Cover

- Does not address specific requirements for implementation of Smart Grid technologies.
- Does not attempt to list all of the available IPS protocols.
- Does not describe how to design a given profile or profiles for networks.
- Does not go into implementation details and specifics about where implementations may have vulnerabilities.

Security References within the IETF Draft Document

Security issues during implementation are mentioned throughout the document and within the protocol sections. For example,

- Section 2.2 describes the following security issues: "While it is popular to complain about the security of the Internet, solutions to many Internet security problems already exist but have either not been widely deployed, may impact critical performance criteria, or require security measures outside the IPS. Internet security solutions attempt to mitigate a set of known threats within the IPS domain at a specified cost; addressing

security issues requires first a threat analysis and assessment and a set of mitigations appropriate to the threats. Since we have threats at every layer, we should expect to find mitigations at every layer." The rest of the section covers physical security, session authentication and confidentiality.

- Section 2.2.1 mentions that physical security is not a protocol issue.
- Section 3.1 documents some security solutions and references existing RFCs that contain more detailed information.

CSWG Conclusions and Recommendations

The CSWG notes that the PAP01 task 2 document does adequately discuss the cyber security requirements which should be considered when implementing the IPS of protocols and does not contain any incorrect statements with regard to cyber security. It further notes that the NISTIR 7628 covers high level cyber security guidelines and should not be considered a reference for this document which covers IETF protocols. Therefore, the CSWG accepts the “Core Protocols in the Internet Protocol Suite” document as fulfilling the PAP01 task 2 requirements with respect to cyber security.

However, the CSWG also recommends the following actions be endorsed by PAP01 and be undertaken by the IETF with respect to cyber security:

- Some IPS core protocols were developed before some of the recent updates to cyber security technologies, and should be reviewed to determine if updates or enhancements are necessary, such as references to cryptographic technologies or more extended network management.
- The normative and informative reference document list in section 8 should be reviewed to determine if any cyber security requirements in those documents need to be updated or enhanced.

Although PAP01 has fulfilled its requirements for describing the cyber security capabilities of the IPS protocols, the CSWG strongly recommends that additional efforts be taken by the SGIP to cover cyber security issues related to implementing the IPS. These could include:

- Enhance the network monitoring and control capabilities of the IPS.
- Complete a set of initial security requirements for different types of networks that are emerging from Smart Grid Use Cases.
- Use the requirements coming from Smart Grid Use Cases as the basis for developing specific profiles using the IPS RFCs.
- Test IPS-based networks for meeting cyber security requirements.

- A version of the NIST IPv6 Profiles document could be developed for the Smart Grid. This suggested approach is similar to that taken by NIST in developing IPv6 Profiles for Federal Agencies.